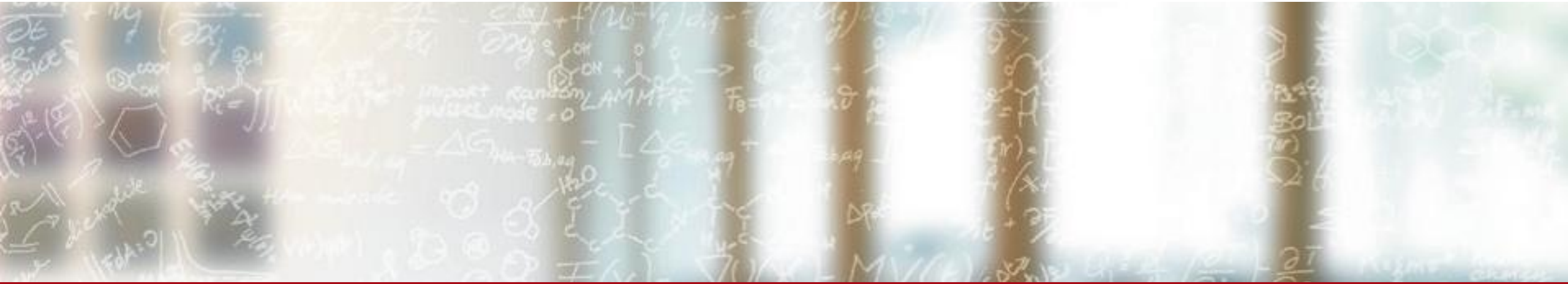**CSCS**
Centro Svizzero di Calcolo Scientifico
Swiss National Supercomputing Centre

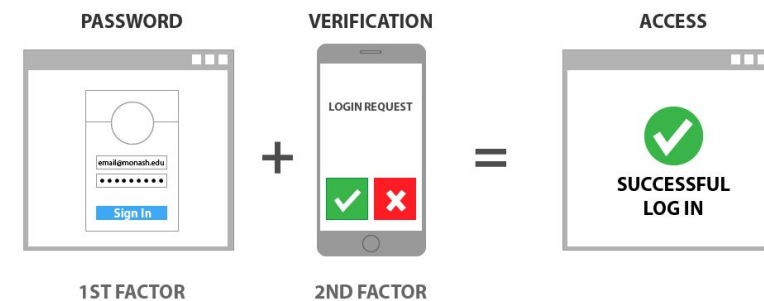**ETH**_zürich_

Multi-factor authentication (MFA) at CSCS

Narendra Challa, CSCS
Dec 05, 2022

What is MFA?

- A digital identity represents a physical person in the digital world

- Connecting a physical person to a digital identity is called authentication

- MFA is a technique to increase the assurance that an authentication is valid

- Authentication was done with one factor such as a login/password pair

- MFA brings more factors to the authentication:
  - Something you know: a login/password, an answer to a private question
  - Something you have: a phone, a card, a USB key,…
  - Something you are: your fingerprint, your facial expression

- At CSCS we implement a 2-factor authentication

PASSWORD   VERIFICATION   ACCESS

email@monash.edu

Sign In

LOGIN REQUEST

✔ ✖

SUCCESSFUL LOG IN

1ST FACTOR   2ND FACTOR

cscs

ETH *zürich*

Why MFA is important?

- Stealing credentials is one of the activities of cyber attackers
  - Use the same password on every web sites ☐ multiple access
  - Simple password to brute force ☐ easy attack

- MFA makes it harder to steal a digital identity
  - It protects better your data and your access to CSCS resources
  - It protects better your research and work

- Follows identity and access management standards
  - Evolution for a better security
  - Evolution for a simpler usage

How does MFA work at CSCS?

- There are 2 authentication mechanisms at CSCS:
    - Web service access: https://xyz.cscs.ch
    - System access: ssh ela.cscs.ch

- Web service access will require to provide a 6-digit code from a device
    - Enrolment process to register a device
    - Digital code asked after entering login/password

- System access will require to use a service for generating special SSH keys
    - Download a SSH key pair from a service https://sshservice.cscs.ch (MFA authentication)
    - Use that key pair to SSH into the frontend node

Web services access

- Enrolment process

  1. You will receive an email informing you that your account is MFA enabled.

  2. You will need to log into any CSCS web service like https://account.cscs.ch by providing your login/password as usual

  3. During the authentication process, you will receive an email to confirm that it was you with a 6 letter-code to enter in the page.

1 Welcome to CSCS MFA

2

Access to CSCS

With CSCS account
- Username myuser
- Password mypwd
- ☐ Remember me

LOG IN

Forgot Password?

With third-party account (beta)
Alternatively, you can sign in using another provider (you still need to have a CSCS account linked to it) Further documentation can be found here

🔍 ETHZ SSO   🔍 FENIX-ACCEPTANCE

🔍 SWITCH EDUID

Help Privacy Terms

Is that you?
Here the code 1A2B3C

3

Access to CSCS

ⓘ Enter the code we sent to your email address.
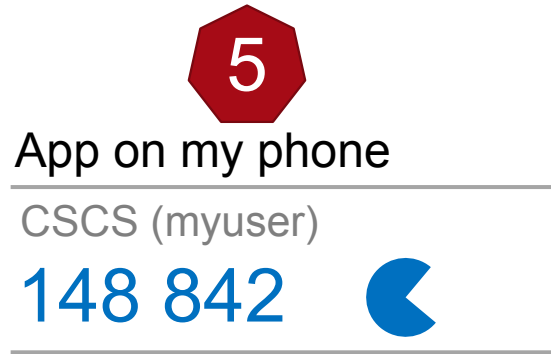
Email verification

🔑 Code 1A2B3C

SUBMIT

Help Privacy Terms

cscs

ETH zürich

Web services access

- ■ Enrolment process
    4. You will need to scan the QR code with app like Google Authenticator to register your device

    5. In the same page you need to enter the 6-digit code provided by the app and a name for your device

    6. Complete!

4

5

App on my phone

CSCS (myuser)

148 842 ◖

Access to CSCS

⚠ You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications on your mobile:
   - ○ FreeOTP
   - ○ Google Authenticator
2. Open the application and scan the QR-code.

Unable to scan?

3. Enter the one-time code provided by the application and click Submit to finish the setup.
   Provide a Device Name to help you manage your OTP devices.

🔑 One-time code   148842

☐ Device Name (not required)   myphone

SUBMIT

Web services authentication with MFA

- Authentication:
  1. Provide your first factor: login and password

  2. Provide the second factor: 6-digit code obtained from your device

  3. Success!

App on my phone

CSCS (myuser)

365 635

System access

- Access to CSCS system is done with SSH

- Once you have been MFA enabled SSH access changes:
  - You CANNOT use login and password.
  - You CANNOT use a key pair that you have generated yourself.
  - You can ONLY use a key pair generated by a CSCS service.
    - This pair of keys are only valid for 24H after that time you need to get a new key pair.
  - Once the keys are downloaded you need to set them in your SSH folder.

- To access the web service you need to authenticate with MFA
  - https://sshservice.cscs.ch

System access - scripts

- We provide a Shell and a Python script to get the keys
- Authenticate
- Retrieve the keys
- Set the keys

```
[sshservice-cli]$ ./cscs-keygen.sh
Username:   myuser
Password:   mypwd
Enter OTP (6-digit code): 365635
Setting the environment : [##########------------------------]
25%  Authenticating to the SSH key service...
Setting the environment : [####################----------------]
50%  Retrieving the SSH keys...
Setting the environment : [##############################----------]
75%  Setting up the SSH keys into your home folder...
Setting the environment : [##############################################]
100%  Completed.

Optional but recommended to set a passphrase on the private key using the
below command:
    $ ssh-keygen -f ~/.ssh/cscs-key –p

 Usage:
    1. Add the key to the SSH agent:
        $ ssh-add ~/.ssh/cscs-key

    2. Connect to the login node using CSCS keys:
        $ ssh -A <CSCS-LOGIN-NODE>


[sshservice-cli]$ ssh –i ~/.ssh/cscs-key ela.cscs.ch
```

cscs

ETH *zürich*

Demo

CSCS

ETH *zürich*

FAQ (1)

1. **I forgot my phone temporarly and cannot authenticate:**
    - Write a ticket to CSCS with the duration of the exception and we will disable MFA for you.

2. **I lost my phone forever and won't be able to authenticate with MFA:**
    - Write a ticket to CSCS and we will reset your MFA, you will need to re-enroll.

3. **I want to change phone, how do I copy the MFA seeds?**
    - Google authenticator allows to transfer seeds, if that does not work we can reset your MFA for you to re-enroll.

4. **Can I register something else than my phone? More than one device?**
    - Yes! However, if your password is stored on your laptop together with your MFA then it lowers security.

FAQ (2)

5. **Can I let my SSH connection open once it has been established?**
   - Yes ☺, we might plan to put a duration limit in the future, but not today.

6. **Can I be exempted from doing MFA?**
   - Mostlikely no, but for some use cases we can grant exceptions.

7. **I have a workflow engine that uses SSH to access systems, can I have an exception?**
   - Not really! The solution is to use FirecREST for your workflow engine or push the provider of the workflow engine to do so.

8. **I offer services using CSCS systems and a service account, what should I do?**
   - Contact us and we will let you create a pair of keys valid for one year with limited scope for your service account.
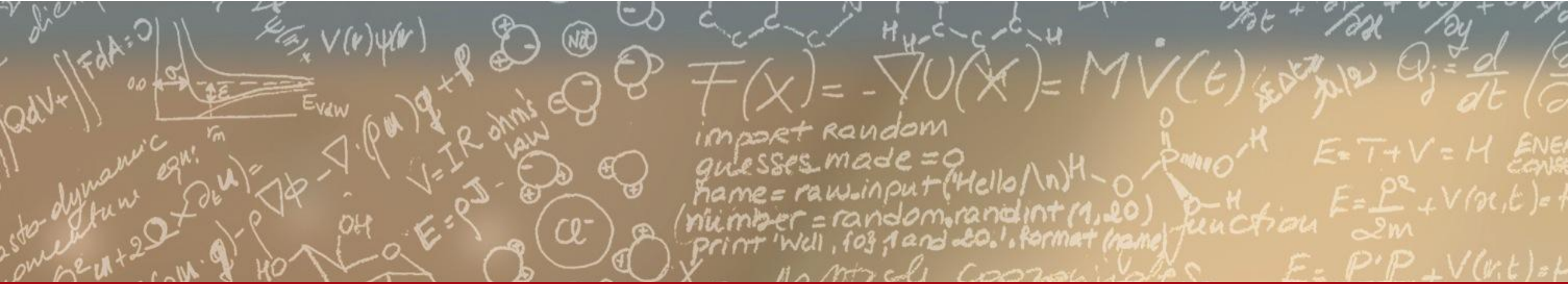
Questions ?

Thank you for your attention.